Beschreibung

Verfahren zur Anmeldung eines mobilen Endgerätes an einem Zugangspunkt eines lokalen Kommunikationsnetzwerkes sowie Zugangspunkt und Endgerät zur Durchführung des Verfahrens

Die Erfindung betrifft ein Verfahren zur Anmeldung eines mobilen Endgerätes an einem Zugangspunkt eines lokalen Kommunikationsnetzwerkes gemäß Anspruch 1, einem Zugangspunkt zur Durchführung des Verfahrens gemäß Anspruch 8 sowie ein Endgerät zur Durchführung des Verfahrens gemäß Anspruch 9.

Die Verschmelzung von Informations- und Kommunikationsnetzen hat dazu geführt, dass Datenübertragungsnetze, wie Lokale Netzwerke LANs, zunehmend mit drahtlosen Zugangspunkten, sogenannten Access Points ausgestattet werden, die es erlauben, neue Netzteilnehmer, auch als Netzknoten bezeichnet, drahtlos an das LAN zu binden. Diese Entwicklung geht sogar soweit, dass zum Teil solche Netze überwiegend bzw. vollständig drahtlos Daten austauschen.

Solcherlei Netze bieten auch Raum für unberechtigte Zugriffe auf Daten innerhalb des Netzes, so dass hierfür vielerlei Ansätze zur Gewährung der Sicherheit entwickelt wurden.

Einer der Ansätze ist die Beschränkung des Datenaustausches innerhalb des Netzes auf bekannte Netzknoten, wobei ein neuer Netzknoten dadurch dem Netz bekannt gemacht wird, dass er bei einem erstmaligen Anmelden, der Erstanmeldung, Authentifizierungsdaten, zumeist Schlüssel zur Verschlüsselung von Daten bei der Übertragung, mit dem jeweiligen Zugangspunkt austauscht.

Ein Nachteil ergibt sich, wenn dieser Austausch drahtlos erfolgt. In diesem Fall kann ein möglicher Angreifer die Authentifizierungsdaten abfangen, um sich für einen unerlaubten

Zugriff als bekanntes Endgerät auszugeben bzw. verschlüsselte Daten mittels der Schlüssel zu entschlüsseln.

Die der Erfindung zugrundeliegende Aufgabe ist, ein Verfahren und eine Anordnung anzugeben, die es erlaubt, unberechtigte Zugriffe auf ein lokales Kommunikationsnetz mit drahtlosen Zugangspunkten weitestgehend zu verhindern.

Diese Aufgabe wird durch das Verfahren ausgehend vom Oberbegriff des Anspruchs 1 durch dessen kennzeichnende Merkmale gelöst. Des Weiteren wird die Aufgabe durch den Zugangspunkt ausgehend vom Oberbegriff des Anspruchs 8 durch dessen kennzeichnende Merkmale sowie durch das Endgerät ausgehend vom Anspruch 9 durch dessen kennzeichnende Merkmale gelöst.

Bei dem erfindungsgemäßen Verfahren zur Erstanmeldung eines, insbesondere mobilen, Endgerätes an einem Zugangspunkt eines lokalen Kommunikationsnetzwerkes nach Anspruch 1 wird eine erste Sendeleistung einer ersten Funksende-/Funkempfangseinrichtung des Zugangspunktes nach Detektieren des Endgerätes derart reduziert, dass ein Sende-/Empfangsvorgang nur in einem Nahfeld des Zugangspunktes erfolgen kann.

Durch das einseitige Senken der ersten Sendeleistung der ersten Funksende-/Funkempfangseinrichtung des Zugangspunktes, so dass ein Empfang nur im Nahfeld des Zugangspunktes möglich ist, wird erreicht, dass Gelegenheiten für ein Mithören mittels eines anderen nicht als zum lokalen Kommunikationsnetz gehörenden Endgerätes (Lauscher) zumindest deutlich reduziert wird. Vor allem wird vermieden, dass ein Lauscher bei der Erstanmeldung üblicherweise übertragene sicherheitsrelevante Daten, wie z.B. Authentifizierungsschlüssel, auswerten kann, da sich ein Lauscher im Allgemeinen nicht im Nahfeld eines Zugangspunktes aufhält und für eine Auswertung sowohl die Daten vom Zugangspunkt als auch die Daten von dem sich zum ersten Mal anmeldenden Endgerät benötigt werden. Ein weiterer Vorteil ist, dass für die Umsetzung dieser Abwehr von Lausch-

angriffen Endgeräte nicht verändert werden müssen, beispielsweise kann die Abwehr auch dann gewährleistet werden, wenn die Endgeräte nicht in der Lage sind, ihre Sendeleistung zu verändern.

Vorteilhafterweise wird bei einer möglichen Weiterbildung der Erfindung nach Detektieren durch den Zugangspunkt eine an das Endgerät gerichtete Signalisierung durchgeführt, welches das Endgerät veranlasst, eine zweite Sendeleistung einer zweiten Funksende-/Funkempfangseinrichtung zu senken, wobei die zweite Sendeleistung derart reduziert wird, dass ein Sende-/Empfangsvorgang nur in einem Nahfeld des Endgerätes erfolgen kann und wobei die Signalisierung vor dem Reduzieren der ersten Sendeleistung erfolgt. Hierdurch wird erreicht, dass weder die vom Zugangspunkt gesendeten Daten noch die von dem Endgerät im Rahmen des Anmeldevorgangs zu sendenden Daten von einem sich außerhalb des Nahfeldes aufhaltenden Lauscher abgefangen werden können, so dass ein Auswerten der ausgetauschten Daten gänzlich verhindert wird.

Vorzugsweise erfolgt die Signalisierung durch Übermittlung einer ersten Nachricht, die für die Angabe eines durch den Zugangspunkt ermittelten empfangenen ersten Signalpegels, insbesondere eines "Received Signal Strength Indicator" RSSI, Wertes vorgesehen ist, wobei anstelle des vorgesehenen ersten Signalpegels ein zweiter, insbesondere einen höheren Wert aufweisender, Signalpegel angegeben wird. Der Vorteil dieser Weiterbildung ist durch die hierdurch mögliche einfachere Implementierung in bereits bestehende Systeme, die zumindest teilweise eine Übertragung über Funk nutzen, gegeben, da im Wesentlichen jeder Funkkommunikationsstandard das Versenden einer derartigen Nachricht als Rückkopplungsinformation für die Quelle des jeweiligen Signals reserviert. Mit dieser Weiterbildung ist es daher möglich, dass Endgeräte ohne Änderungen das erfindungsgemäße Verfahren unterstützen können. Lediglich die Zugangspunkte müssen derart ausgestaltet sein, dass sie diese gemäß Funkkommunikationsstandards reservierte

Nachricht für einen anderen Zweck nutzen, d.h. unabhängig von der Höhe des tatsächlich empfangenen Signalpegels einen derart hohen empfangenen Signalpegel zu signalisieren, dass das Endgerät (Quelle) seine Sendeleistung auf ein Maß reduziert, dass ein Datenempfang nur in einem Nahfeld des Endgerätes möglich ist.

Enthält die Signalisierung eine zweite Nachricht, die das Endgerät zur Ausgabe eines Hinweises an den Nutzer des Endgerätes dahingehend auffordert, das Endgerät in das Nahfeld des Zugangspunktes zu bringen, wird vermieden, dass ein Datenaustausch zur Umsetzung der Erstanmeldung des Endgerätes dadurch ungewollt unterbrochen wird, dass ein Nutzer des Endgerätes keine Kenntnis darüber hat, dass er sich mit dem Endgerät zur Erstanmeldung im Nahfeld des Zugangspunktes aufhalten muss.

Um sicherzustellen, dass die zweite Nachricht den gewünschten Effekt - das Inkenntnissetzen des Nutzer - erzielt, wird die zweite Nachricht bei einer Weiterbildung nach Ablauf einer vorbestimmten Zeitspanne erneut gesendet, wobei zur Sicherstellung, dass diese Nachricht vom Endgerät empfangen werden kann, zumindest vorübergehend die erste Sendeleistung auf einen zum Zeitpunkt der Detektion bestehenden Pegel erhöht wird.

Vorstellbar ist es auch, dass das erneute Senden periodisch jeweils nach Ablauf der vorbestimmten Zeitspanne wiederholt wird, so dass mit einer höheren Wahrscheinlichkeit ausgeschlossen werden kann, dass der Nutzer die Nachricht nicht zur Kenntnis genommen hat.

Funktioniert die erste und zweite Funksende-/Funkempfangseinrichtung gemäß einem Kurzstreckenfunkstandard, so wird die bei diesem Standard ohnehin schon kurze Übertragungsdistanz noch verringert, so dass ein Lauscher gesehen wird, wenn er versucht, sich ins durch die erste und zweite Funksende-/Funkempfangsrichtung funkversorgte Nahfeld zu begeben. Zudem

weisen Funksende-/Funkempfangseinrichtungen neuerer Entwicklungsgenerationen, insbesondere nach dem Bluetooth-Standard funktionierende Funksende-/Funkempfangseinrichtungen, Chipsätze auf, die eine Variation der Sendeleistung in einem Endgerät erlauben.

Der erfindungsgemäße Zugangspunkt gemäß Anspruch 8 sowie das erfindungsgemäße Endgerät gemäß Anspruch 9 zeichnen sich durch Mittel zur Durchführung des Verfahrens aus, so dass das erfindungsgemäße Verfahren in den entsprechenden Geräten Unterstützung findet.

Weitere Einzelheiten und Vorteile der Erfindung werden in den Figuren 1 bis 2 erläutert. Davon zeigen

Figur 1 Darstellung eines Anordnungsszenarios, bei dem ein Versuch eines Lauschangriffs möglich wäre,

Figur 2 ein Ablaufdiagramm des erfindungsgemäßen Verfahrens bei einem Einsatz in einer Anordnung gemäß dem Szenario.

In Figur 1 ist beispielhaft eine Anordnung gezeigt, die erfindungsgemäß einen Versuch eines Lauschangriffs durch ein zum Lauschen verwendetes Endgerät LA abwehrt, wobei dies dadurch erreicht wird, dass sich ein einem lokalen Netzwerk LAN noch nicht bekanntes Endgerät, welches bei dem dargestellten Ausführungsbeispiel gemäß dem Bluetooth-Standard funktioniert, in einem ersten Funkversorgungsbereich N1 eines Zugangspunktes (Access Point) AP des lokalen Netzwerks LAN befindet.

Dieser erste Funkversorgungsbereich N1 wird von einer ersten Funksende-/Funkempfangseinrichtung TRX1 bereitgestellt, wobei eine erste Sendeleistung der ersten Funksende-/Funkempfangseinrichtung TRX1 einen von einem ersten Mikroprozessor µP1 geregelten Wert aufweist, der die Reichweite des ersten Funk-

versorgungsbereiches N1 auf ein Nahfeld des Access Points AP begrenzt, d.h. einen Radius aufweist, der im Allgemeinen wenige Dezimeter, alternativ auch bis zu einem Meter, beträgt.

Neben dem ersten Funkversorgungsbereich N1, ist bei diesem Ausführungsbeispiel auch der zweite Funkversorgungsbereich N2 eines neu anzumeldenden Endgerätes PC auf ein Nahfeld im Allgemeinen gleicher Reichweite wie der Reichweite des ersten Funkversorgungsbereiches N2 begrenzt. Dies wird durch Regelung einer zweiten Sendeleistung einer zweiten Funksende-/Funkempfangseinrichtung TRX2 des Endgerätes PC durch einen zweiten Mikroprozessor µP2 (Bluetooth-Chipsatz) erreicht.

Innerhalb des zweiten Funkversorgungsbereiches N2 befindet sich der Access Point AP, so dass eine Datenübertragung in beiden Richtungen problemlos möglich ist, wobei der Versuch eines Lauschangriffes durch ein anderes nicht gemeldetes Endgerät LA verhindert bzw. zumindest erschwert wird, dass es sich nicht innerhalb beider künstlich begrenzter Funkversorgungsbereiche N1, N2 befindet.

Eine Erstanmeldung, die gemäß Bluetooth Standard als "Pairing Prozess" bezeichnet wird, ist besonders kritisch, da sich bei diesem Prozess ein Bluetooth-Endgerät durch Übertragung von Schlüsseln einmalig bei einem Netz authentifiziert und damit fortan als bekanntes vertrauenswürdiges Endgerät "trusted device" gespeichert wird, so dass ein Abfangen dieser Information (Schlüssel) einem Lauscher die Möglichkeit für weitere unberechtigte Zugriffe auf das Netz ermöglichen würde.

Die in Figur 1 gezeigte Anordnung wehrt derartige Angriffe durch das Ausführungsbeispiel des erfindungsgemäßen Verfahrens, dessen Ablaufdiagramm in Figur 2 dargestellt ist, ab.

Das in der Figur 2 dargestellte Ablaufdiagramm zeigt die im Rahmen des erfindungsgemäßen Verfahrens durchzuführenden Schritte in dem oben beschriebenen Szenario.

Das Verfahren beginnt im Allgemeinen damit, dass durch den Access Point AP ein unbekanntes Endgerät PC detektiert wird und sich der Access Point AP somit in einem ersten Schritt S1 im Zustand "Unbekanntes Bluetooth Endgerät" befindet.

Ausgehend von diesem ersten Schritt S1 wird anschließend dem Bluetooth-Endgerät PC in einem folgenden zweiten Schritt S2 im Allgemeinen ein künstlich überhöhter empfangener Signalpegel signalisiert (RSSI-Wert). Künstlich überhöht bedeutet hierbei, dass im Allgemeinen nicht der tatsächlich ermittelte Signalpegelwert signalisiert wird, sondern erfindungsgemäß ein derart hoher Wert, dass das Endgerät PC seine Sendeleistung auf ein Niveau senkt, welches zu einem zweiten Funkversorgungsbereich N2 des Endgerätes PC führt, der auf ein Nahfeld begrenzt ist.

Wird das Verfahren in einem Funksystem eingesetzt, welches Endgeräte aufweist, die keine Regelung der Sendeleistung unterstützen, kann der zweite Schritt S2 ausbleiben. Alternativ ist es auch denkbar, dass der zweite Schritt S2 bewusst durchgeführt wird, selbst wenn es sich um ein Endgerät PC handeln würde, das keine Regelung unterstützt. In diesem Fall wird der Abhörschutz allein dadurch gewährleistet, dass der Zugangspunkt AP in einem dritten Schritt S3 seine Sendeleistung auf einen Wert reduziert, der den ersten Funkversorgungsbereich N1 auf ein Nahfeld begrenzt.

Unterstützt dagegen das Endgerät PC eine Regelung der Sendeleistung - wie für dieses Ausführungsbeispiel angenommen - so wird sowohl durch das Reduzieren der Sendeleistung des Zugangspunktes AP im dritten Schritt S3 als auch durch Reduzieren der Sendeleistung des Endgerätes PC in einem vierten Schritt S4 die Abwehr eines möglichen Lauschers LA gewährleistet.

Im Anschluss hieran erfolgt in einem fünften Schritt S5 ein Überprüfen, ob sich das Endgerät PC in Reichweite der ersten Funksende-/Funkempfangsvorrichtung TRX1 des Access Points AP befindet, wobei dies beispielsweise dadurch realisiert wird, dass keine Antwort seitens des Endgerätes PC an den Zugangspunkt übermittelt wird.

Dieser fünfte Schritt S5 wird in einer Schleife solange wiederholt, d.h. Anfragen an das Endgerät PC gesendet, bis eine Antwort empfangen wird, so dass klar ist, dass das Endgerät sich im Nahfeld des Zugangspunktes befindet.

Um dies zu beschleunigen bzw. zu unterstützen, kann alternativ bzw. ergänzend mit der Signalisierung im zweiten Schritt auch eine Nachricht übermittelt werden, die das Endgerät PC veranlasst, seinem Nutzer einen Hinweis darauf zu geben, dass er sich mit dem Endgerät für diesen Pairing Prozess in das Nahfeld des Zugangspunktes AP begeben muss.

Alternativ kann in Verbindung mit dem fünften Schritt diese Aufforderung erstmalig erfolgen und/oder nach jedem negativen Detektionsergebnis periodisch wiederholt werden, um dem Nutzer eine Rückkopplung darüber zu geben, dass er evtl. noch nicht nahe genug am Zugangspunkt AP ist.

Ergibt das Detektieren im fünften Schritt S5, dass sich das Endgerät PC im Nahfeld des Access Points AP befindet, wie in Figur 1 dargestellt, so kann in einem sechsten Schritt S6 mit dem eigentlichen Pairing Prozess begonnen werden und das erfindungsgemäße Verfahren beendet werden.

Patentansprüche

1. Verfahren zur Erstanmeldung eines, insbesondere mobilen, Endgerätes (PC) an einem Zugangspunkt (AP) eines lokalen Kommunikationsnetzwerkes (LAN), dadurch gekennzeichnet, dass eine erste Sendeleistung einer ersten Funksende-/Funkempfangseinrichtung (TRX1) des Zugangspunktes (AP) nach Detektieren (S1) des Endgerätes (PC) derart reduziert wird (S3), dass ein Sende-/Empfangsvorgang nur in einem Nahfeld des Zugangspunktes (AP) erfolgen kann.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass nach Detektieren durch den Zugangspunkt eine an das Endgerät (PC) gerichtete Signalisierung durchgeführt wird, welches das Endgerät (PC) veranlasst, eine zweite Sendeleistung einer zweiten Funksende-/Funkempfangseinrichtung (TRX2) zu senken (S2), wobei die zweite Sendeleistung derart reduziert wird, dass ein Sende-/Empfangsvorgang nur in einem Nahfeld des Endgerätes (PC) erfolgen kann und wobei die Signalisierung vor dem Reduzieren der ersten Sendeleistung erfolgt.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Signalisierung durch Übermittlung einer ersten Nachricht, die für die Angabe eines durch den Zugangspunkt (AP) ermittelten empfangenen ersten Signalpegels, insbesondere eines "Receivied Signal Strength Indicator" RSSI, Wertes vorgesehen ist (S2), erfolgt, wobei anstelle des vorgesehenen ersten Signalpegels ein zweiter, insbesondere einen höheren Wert aufweisender, Signalpegel angegeben wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Signalisierung (S2) eine zweite Nachricht enthält, die das Endgerät (PC) zur Ausgabe eines Hinweises an den Nutzer des Endgerätes (PC)

dahingehend auffordert, das Endgerät (PC) in das Nahfeld des Zugangspunktes (AP) zu bringen.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Nachricht nach Ablauf einer vorbestimmten Zeitspanne erneut gesendet wird, wobei hierzu zumindest vorübergehend die erste Sendeleistung auf einen zum Zeitpunkt der Detektion bestehenden Pegel erhöht wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass das erneute Senden periodisch jeweils nach Ablauf der vorbestimmten Zeitspanne wiederholt wird (S5).

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die erste und zweite Funksende-/Funkempfangseinrichtung (TRX1, TRX2) gemäß einem Kurzstreckenfunkstandard, insbesondere nach dem Bluetooth-Standard, funktioniert.

8. Zugangspunkt (AP), insbesondere nach einem der vorhergehenden Ansprüche 1 bis 6, gekennzeichnet durch Mittel (µP1, TRX1) zur Durchführung des Verfahrens.

9. Endgerät (PC), insbesondere nach einem der Ansprüche 1 bis 6, gekennzeichnet durch Mittel (µP2, TRX2) zur Durchführung des Verfahrens.

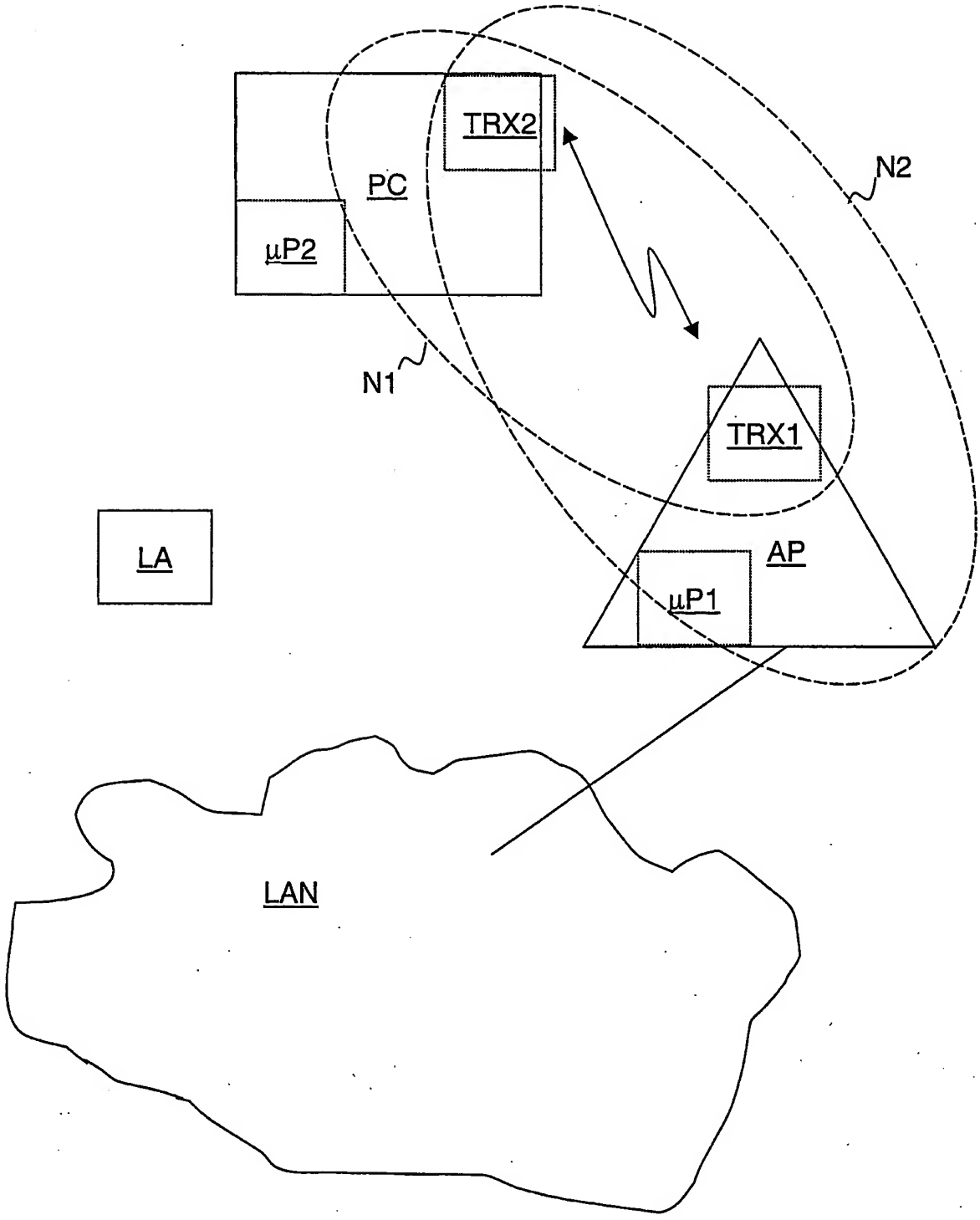

FIG 1

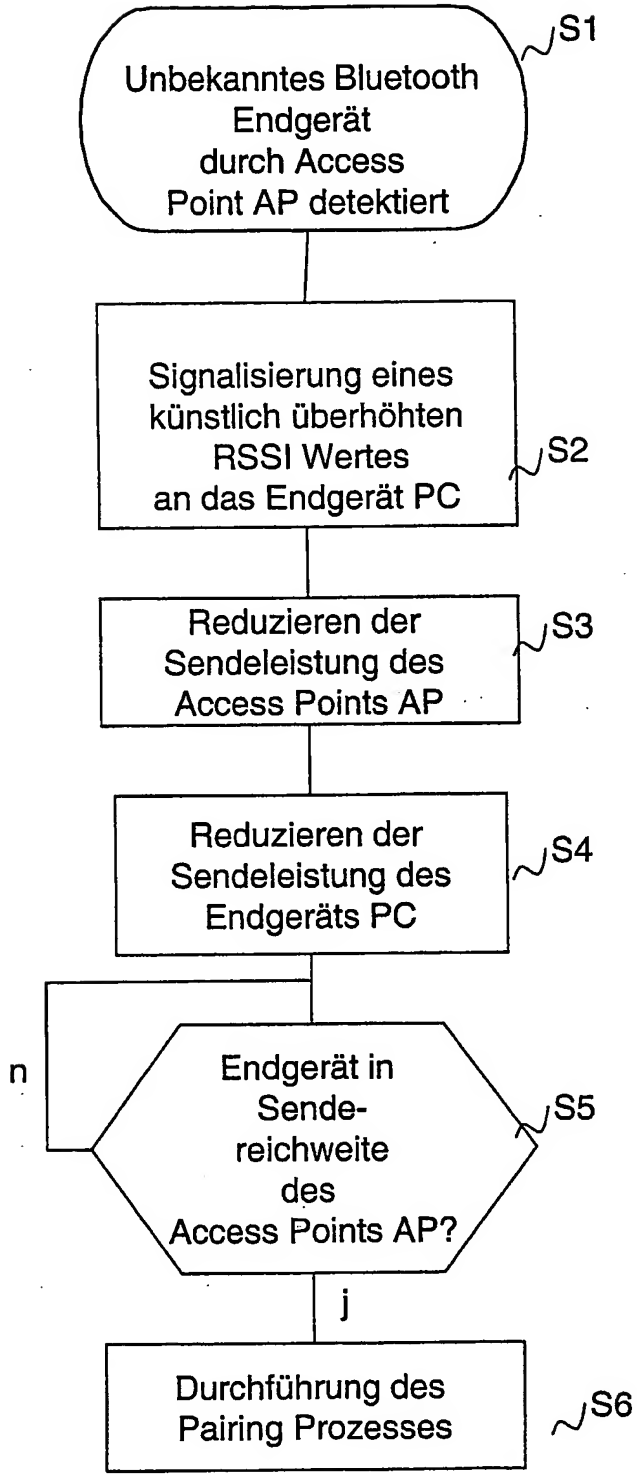

FIG 2